

12 **EUROPÄISCHE PATENTANMELDUNG**

21 Anmeldenummer: 89105509.7

51 Int. Cl. 4: **G07F 7/10**

22 Anmeldetag: 29.03.89

30 Priorität: 11.04.88 CH 1323/88

43 Veröffentlichungstag der Anmeldung:
18.10.89 Patentblatt 89/42

84 Benannte Vertragsstaaten:
AT BE CH DE ES FR GB IT LI NL SE

71 Anmelder: **SPA Syspatronic AG**
Industriestrasse 31 Postfach 2066
CH-6302 Zug(CH)

72 Erfinder: **Schwartz, Hermann**
Schützenstrasse 18
CH-8808 Pfäffikon(CH)

74 Vertreter: **Kägi, Otto**
Patentanwalt Hinterbergstrasse 36 Postfach
CH-6330 Cham(CH)

54 **Tragbare Datenträgeranordnung.**

57 Bei tragbaren Datenträgeranordnungen, die zum bedarfsweisen Anschluss (z. B. über Kontakte 9) an eine externe Schreib- und Leseinheit in einem Datenaustauschsystem bestimmt sind und die ausser einer Steuereinheit (2) einen zusätzlichen Datenspeicher (4) enthalten (beides als integrierte Schaltung ausgeführt), soll eine hohe Sicherheit vor Zugriff auf gespeicherte Daten und Manipulationen durch Unbefugte erreicht werden. Zu diesem Zweck wird die Ansteuerung des zusätzlichen Datenspeichers (5) von der Steuereinheit (2) her geschützt. Es sind verschiedene Möglichkeiten wie Zugriffs-Codierung, kryptografische Schaltungsmittel und Verfahren oder geheimer Mikrocode angegeben. Ausführung der Datenträgeranordnung (1) mit zwei oder mehreren separaten, durch Leiterbahnen (3) verbundenen integrierten Schaltungsbausteinen (multi chip), oder mit allen Funktionseinheiten integriert auf einem gemeinsamen Träger (single chip).

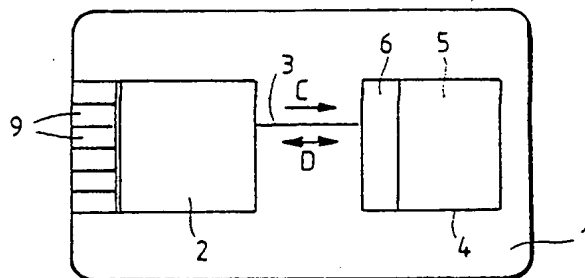


Fig. 1

Tragbare Datenträgeranordnung

Die Erfindung betrifft eine tragbare Datenträgeranordnung, enthaltend eine Steuereinheit und einen zusätzlichen Datenspeicher, die je als integrierte Schaltung ausgeführt sind, wobei die Steuereinheit mit Mitteln zur Verbindungsherstellung zu einer externen Schreib- und Leseinheit versehen ist.

Es sind Datenaustausch- und -verarbeitungssysteme mit einer Vielzahl solcher tragbarer Datenträgeranordnungen bekannt, die von individuellen Benützern nach Bedarf mit einer Schreib- und Leseinheit in Verbindung gebracht werden, um mit dem System zu kommunizieren. Datenträgeranordnungen der genannten Art, die neben ausreichender Speicherkapazität mit einer Steuereinheit ausgestattet sind, ermöglichen nicht nur einen interaktiven Daten- und Signalaustausch mit dem System, sondern eine dezentralisierte Datenverarbeitung und -speicherung in den individuellen, "intelligenten" Datenträgeranordnungen, wodurch sich äusserst vielfältige und hochentwickelte Anwendungsmöglichkeiten ergeben. Solche Datenträgeranordnungen werden typischerweise in Kartenform (im Kreditkartenformat) mit eingelagerten integrierten Schaltungsbausteinen ausgeführt (sogenannte "Chipkarten"); wenn deshalb nachstehend vorwiegend von Datenträger-"Karten" die Rede ist, sollen jedoch andere Ausgestaltungen keinesfalls ausgeschlossen werden.

Bei fast allen Anwendungen solcher Datenaustauschsysteme ist eine der wichtigsten Voraussetzungen die Sicherheit vor Manipulationen und missbräuchlichem bzw. unbefugtem Zugriff auf gespeicherte und übermittelte Informationen, sowohl bei den "festen" Systemkomponenten wie auch bei den tragbaren Datenträgern. Hohe Sicherheitsanforderungen bestehen bei den letzteren insbesondere wegen ihrer grossen Verbreitung (Möglichkeit des Verlierens oder Entwendens), aber auch - bei "eingebauter Intelligenz" - wegen der Vielzahl von darin gespeicherten Daten sowie gespeicherten elektronischen Verschlüsselungen, wie sie für den geschützten Datenverkehr mit Schreib- und Leseeinheiten benötigt werden (Identifikations- und Authentifikationsfunktionen).

Aufgabe der vorliegenden Erfindung ist deshalb die Sicherung tragbarer Datenträger der genannten Art gegen Zugriff und Entschlüsselung bzw. Interpretation von darin gespeicherten sicherheitsrelevanten Daten und Informationen durch unbefugte Dritte. Diese Aufgabe wird erfindungsgemäss dadurch gelöst, dass in der genannten Datenträgeranordnung die Ansteuerung des zusätzlichen Datenspeichers von der Steuereinheit her geschützt ist. Das geschützte Ansteuern lässt sich - wie

weiter unten beschrieben - auf verschiedene Weise durch integrierte kryptografische Schaltungsmittel oder Verfahren verwirklichen. Dadurch wird in den einzelnen Datenträgeranordnungen ein missbräuchlicher Zugriff wirksam verhindert.

Bestimmte geeignete Varianten der Erfindung sind in den Ansprüchen 2 bis 7 angegeben. Besonders ist darauf hinzuweisen, dass die Erfindung unabhängig davon anwendbar ist, ob die integrierten Schaltungen einer Datenträgeranordnung ("Karte") in zwei oder mehrere, durch Leitungen verbundene Bausteine aufgeteilt oder auf einem einzigen Träger vereint sind (sogenannte multi chip- oder single chip-Ausführung). Die Erfindung ermöglicht also die Ausdehnung der Speicherkapazität auf zusätzliche Chips wie auch die Anwendung komplexerer Chips unter Wahrung der "inneren" Sicherheit der Datenträgeranordnung.

Weitere Merkmale der Erfindung ergeben sich aus der nachstehenden Beschreibung verschiedener Ausführungsbeispiele in Verbindung mit der Zeichnung.

Die Figuren 1 bis 4 sind schematische Darstellungen von Datenträgerkarten, insbesondere Plastikkarten mit eingebetteten integrierten Halbleiterschaltungen ("Chips"), wobei die letzteren in Bezug auf das Kartenformat stark vergrössert und vereinfacht mit darauf angeordneten Schaltungs- bzw. Funktionsbereichen dargestellt sind. Selbstverständlich wird das Layout dieser Schaltungen - Ausdehnung und Gestalt der einzelnen Bereiche - je nach Anwendung verschieden sein.

In Fig. 1 ist als Datenträgeranordnung eine Plastikkarte 1 dargestellt, in welcher zwei integrierte Halbleiter-Schaltungsbausteine ("Chips") 2 und 4 gebettet sind. Der Baustein 2 enthält die Steuereinheit der Datenträgeranordnung und ist zwecks Verbindung zu einer externen, nicht dargestellten Schreib- und Leseinheit eines Datenaustauschsystems an Aussenkontakte 9 der Karte 1 angeschlossen; die Verbindungsherstellung zur externen Einheit kann auch auf andere Weise als über galvanische Kontakte erfolgen, beispielsweise wie an sich bekannt mittels induktiver Ankopplung usw. Die Steuereinheit 2 enthält vorzugsweise einen Mikroprozessor mit Rechenwerk und RAM- und ROM-Speicherbereichen sowie ferner einen Datenspeicherbereich. Ein zusätzlicher Datenspeicher 5 befindet sich auf dem zweiten Baustein 4. Die Verbindung zwischen den Bausteinen 2 und 4 ist über eine Anzahl Leiterbahnen 3 hergestellt. Aus herstellungstechnischen Gründen kann es zweckmässig sein, die Bausteine 2 und 4 mit den Leiterbahnen 3 und gegebenenfalls Aussenkontakten 5 für den Einbau in die Plastikkarte 1 zu einem gemeinsamen

Modul zusammenzufassen.

Eine externe Verbindung kann nur von der Steuereinheit 2 aus über die Kontakte 5 hergestellt werden, wobei ein Austausch sicherheitsrelevanter Daten zwischen Karte und System in an sich bekannter Weise erst nach erfolgreicher Authentikation und Identifikation zustande kommen kann, an welchen Funktionen die Steuereinheit beteiligt ist. Ein Datenaustausch erfolgt jedoch auch "kartenintern" zwischen den Bausteinen 2 und 4 über die Leiterbahnen 3. Um Manipulationen und unbefugten Zugriff zu den Daten im zusätzlichen Datenspeicher 5 zu verhindern, ist die Ansteuerung dieses Speichers von der Steuereinheit 2 her geschützt. Beim Beispiel nach Fig. 1 ist zu diesem Zweck dem Datenspeicher 5 ein Zugriffs-Codebereich 6 zugeordnet, wodurch der Speicher nur über Codesignale C, die von der Steuereinheit 2 erzeugt werden, ansteuerbar ist, d.h. ein Datenaustausch D zwischen den Bausteinen 2 und 4 ist nur nach erfolgter Entschlüsselung über den Codebereich 6 möglich. Auch ein Datenaustausch innerhalb des Bausteins 2 zwischen der Steuereinheit und einem dort vorhandenen Datenspeicher erfolgt, wie nicht weiter dargestellt, auf ähnlich geschützter Weise. Solche geschützten Datenaustausch-Vorgänge erfolgen innerhalb der Datenträgeranordnung 1 gewissenmaßen autark ohne Beteiligung externer Systemteile (abgesehen natürlich von der Stromversorgung über Kontakte 9). Der Zugriff insbesondere zu sicherheitsrelevanten Daten im Datenspeicher 5 ist somit durch eine Sperre geschützt, welche nur mittels innerhalb der Karte verwendeten Schlüsselcodes (key lock) überwunden werden kann. Dabei kann die Sicherheit noch dadurch wesentlich gesteigert werden, dass im Mikroprozessor der Steuereinheit 2 immer neue geheime Zugriffs-Codes generiert werden, z.B. nach jedem erfolgten Zugriff auf den zusätzlichen Datenspeicher.

Zweckmäßigerweise werden die Datenspeicher als elektrisch schreib- und löschbare Speicher ausgeführt (sogenannte EEPROM-Speicher). Die Ausführung des zusätzlichen Datenspeichers 5 als serieller Speicher mit Vergleichslogik ermöglicht, mit einer geringen Zahl von Verbindungsleitungen 3 zwischen den Bausteinen 2 und 4 auszukommen.

Beim Ausführungsbeispiel nach Fig. 2 ist der generelle Aufbau der Datenträgerkarte 1 mit integrierter Schaltungsbausteinen 2a, 4a, die über Leiterbahnen 3 verbunden sind, gleich wie bei Fig. 1. Die mit Aussenkontakten 9 verbundene Steuereinheit 2a enthält wiederum einen Mikroprozessor und einen Datenspeicher-Bereich. Der Baustein 4a enthält dagegen ausser dem zusätzlichen Datenspeicher 5 ebenfalls einen Mikroprozessor 8, wodurch sich erweiterte Möglichkeiten hinsichtlich Anwendung und Sicherheit ergeben. Mit Hilfe des Mikroprozessors 8 ist es möglich, nicht nur wie bei Fig.

1 die Ansteuerung des Datenspeichers 5 von der Steuereinheit 2 her zu schützen und damit das unbefugte Auslesen von Daten aus dem Speicher 5 zu verhindern, sondern darüber hinaus den gesamten Datenaustausch über die Leitungen 3 zu sichern, d.h. in codierter oder verschlüsselter Form durchzuführen. Die beidseitige Ansteuerung ist jeweils nur nach erfolgreicher gegenseitiger kryptografischer Authentikation möglich, die wiederum nur "kartenintern", d.h. ohne Beteiligung externer Systemteile erfolgt.

Der generelle Aufbau beim Beispiel nach Fig. 3 mit Steuereinheit 2b und zusätzlichem Datenspeicher 4b in Form von separaten integrierten Schaltungen entspricht wiederum den vorangehenden Beispielen. Eine geschützte Ansteuerung des zusätzlichen Datenspeichers 5 wird hier indessen nochmals auf eine andere Weise verwirklicht, nämlich dadurch, dass der Mikrocode der Steuereinheit 2b, durch 10 angedeutet, geheim ist. Es kann zwar in der Steuereinheit 2b ein an sich bekannter Mikroprozessor verwendet werden, welcher jedoch auf einem "unüblichen", nur dem Hersteller bekannten und damit geheimen Mikrocode 10 beruht. Dadurch wird ein unbefugter Zugriff auf im Datenträger gespeicherte Daten bzw. die Entschlüsselung von über die Leitungen 3 ausgetauschten Informationen verunmöglicht, auch wenn es gelingen sollte, die Leiterbahnen 3 freizulegen.

Im Gegensatz zu den vorangehend beschriebenen Ausführungsbeispielen enthält die Datenträgeranordnung bzw. die Plastikkarte 1 nach Fig. 4 einen einzigen Halbleiterbaustein 12, auf welchem die Steuereinheit 2c, der zusätzliche Datenspeicher 5 sowie weitere Schaltungsbereiche insgesamt in integrierter Schaltungsbauweise ausgeführt sind. Ähnlich wie beim Beispiel nach Fig. 3 ist im Mikroprozessor der Steuereinheit 2c der Mikrocode 10a geheim, so dass die Ansteuerung des zusätzlichen Datenspeichers 5 wiederum geschützt ist (ein "mechanischer" Zugriff auf Leitungen zwischen Bereichen der integrierten Schaltung auf einem und demselben Träger wäre natürlich noch erheblich schwieriger als auf Leitungen 3, welche innerhalb der Plastikkarte 1 verlegt sind bzw. innerhalb eines Moduls, welcher zwei getrennte Bausteine 2 und 4 umfasst).

Mit dem Rechenwerk im Mikroprozessor der Steuereinheit 2c steht ferner ein zusätzliches Rechenwerk 14 mit Registern 15 in Verbindung, die ebenfalls auf dem Träger 12 angeordnet sind. Wie angedeutet, sind die Register 15 ebenfalls auf den geheimen Mikrocode 10a der Steuereinheit 2c ausgerichtet, d.h. der Signalaustausch zwischen der Steuereinheit 2c und dem zusätzlichen Rechenwerk 14 erfolgt ebenfalls aufgrund des geheimen Codes. Ein solches zusätzliches Rechenwerk 14 ermöglicht die Durchführung besonders hochent-

wickelter kryptografischer Verfahren innerhalb der tragbaren Datenträgeranordnung, d.h. ohne Beanspruchung externer Rechenkapazität und dadurch bedingtem Datenaustausch mit externen Systemteilen. Dies bedeutet, dass die Anwendung des geheimen Mikrocodes 10a auf die integrierte Schaltung des einzigen Trägers 12 in der Datenträgeranordnung beschränkt bleibt, wodurch eine extreme Sicherheit vor Manipulation und unbefugtem Zugriff erzielt wird.

5

10

Ansprüche

1. Tragbare Datenträgeranordnung, enthaltend eine Steuereinheit und einen zusätzlichen Datenspeicher, die je als integrierte Schaltung ausgeführt sind, wobei die Steuereinheit mit Mitteln zur Verbindungsherstellung zu einer externen Schreib- und Leseinheit versehen ist, dadurch gekennzeichnet, dass die Ansteuerung des zusätzlichen Datenspeichers (5) von der Steuereinheit (2) her geschützt ist.

15

20

2. Tragbare Datenträgeranordnung nach Anspruch 1, dadurch gekennzeichnet, dass der Datenspeicher (5) einen Zugriffs-Codebereich (6) enthält und über von der Steuereinheit (2) erzeugte Codesignale (C) ansteuerbar ist.

25

3. Tragbare Datenträgeranordnung nach Anspruch 1, dadurch gekennzeichnet, dass dem Datenspeicher (5) ein Prozessor (8) zum gesicherten (codierten oder verschlüsselten) Datenaustausch mit der Steuereinheit (2a) zugeordnet ist.

30

4. Tragbare Datenträgeranordnung nach Anspruch 1, dadurch gekennzeichnet, dass der Mikrocode (10) der Steuereinheit (2b) geheim ist.

35

5. Tragbare Datenträgeranordnung nach Anspruch 1, dadurch gekennzeichnet, dass mit dem Rechenwerk der Steuereinheit (2c) ein zusätzliches Rechenwerk (14) in Verbindung steht, dessen Register (15) auf den Mikrocode (10a) der Steuereinheit (2c) ausgerichtet ist bzw. sind.

40

6. Tragbare Datenträgeranordnung nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass Steuereinheit und zusätzlicher Datenspeicher als separate integrierte Schaltungen (2, 4) ausgeführt sind, welche durch Leiterbahnen (3) innerhalb der Datenträgeranordnung (1) miteinander verbunden sind.

45

7. Tragbare Datenträgeranordnung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass Steuereinheit (2), zusätzlicher Datenspeicher (5) samt weiteren Bereichen (6, 8, 14, 15) insgesamt in integrierter Schaltungsbauweise auf demselben Träger (12) ausgeführt sind.

50

55

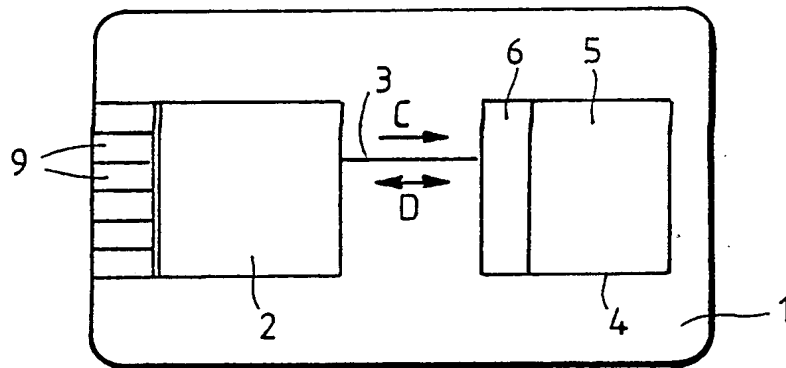


Fig. 1

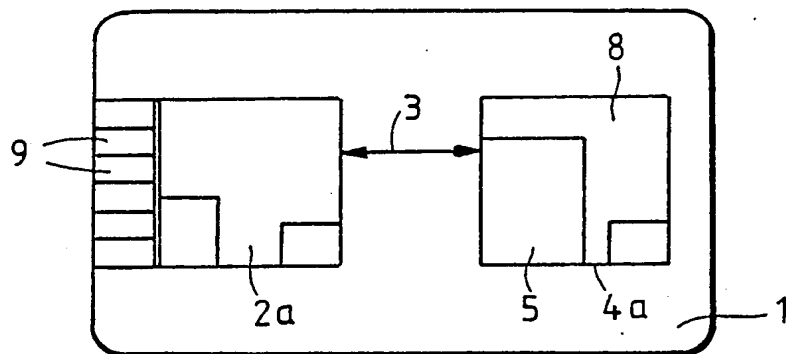


Fig. 2

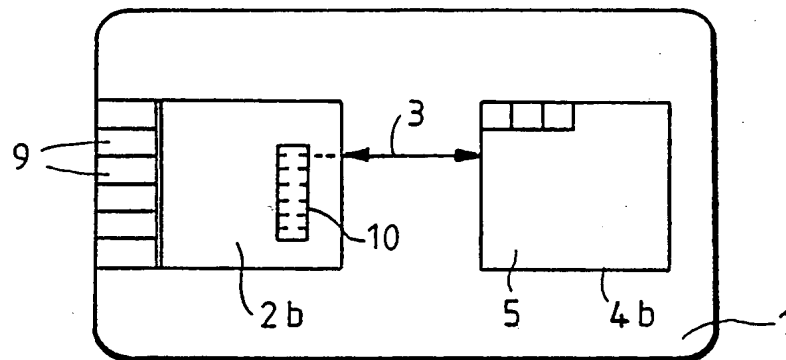


Fig. 3

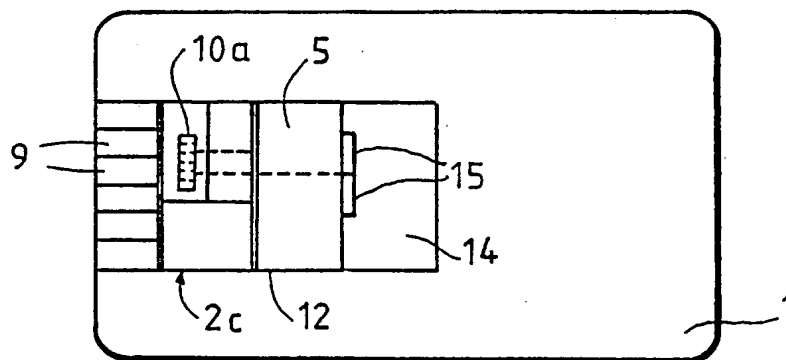


Fig. 4



Europäisches Patentamt
European Patent Office
Office européen des brevets



Veröffentlichungsnummer: **0 337 185 A3**

(2)

EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: 89105509.7

(51) Int. Cl.⁵ G07F 7/10

(22) Anmeldetag: 29.03.89

(30) Priorität: 11.04.88 CH 1323/88

(43) Veröffentlichungstag der Anmeldung:
18.10.89 Patentblatt 89/42

(34) Benannte Vertragsstaaten:
AT BE CH DE ES FR GB IT LI NL SE

(83) Veröffentlichungstag des später veröffentlichten
Recherchenberichts: 27.03.91 Patentblatt 91/13

(71) Anmelder: SPA Syspatronic AG
Industriestrasse 31 Postfach 2066
CH-6302 Zug(CH)

(72) Erfinder: Schwartz, Hermann
Schützenstrasse 18
CH-8808 Pfäffikon(CH)

(74) Vertreter: Kägi, Otto
Patentanwalt Hinterbergstrasse 36 Postfach
CH-6330 Cham(CH)

(54) Tragbare Datenträgeranordnung.

(57) Bei tragbaren Datenträgeranordnungen, die zum bedarfsweisen Anschluss (z. B. über Kontakte 9) an eine externe Schreib- und Leseinheit in einem Datenaustauschsystem bestimmt sind und die ausser einer Steuereinheit (2) einen zusätzlichen Datenspeicher (4) enthalten (beides als integrierte Schaltung ausgeführt), soll eine hohe Sicherheit vor Zugriff auf gespeicherte Daten und Manipulationen durch Unbefugte erreicht werden. Zu diesem Zweck wird die Ansteuerung des zusätzlichen Datenspeichers (5)

von der Steuereinheit (2) her geschützt. Es sind verschiedene Möglichkeiten wie Zugriffs-Codierung, kryptografische Schaltungsmittel und Verfahren oder geheimer Mikrocode angegeben. Ausführung der Datenträgeranordnung (1) mit zwei oder mehreren separaten, durch Leiterbahnen (3) verbundenen integrierten Schaltungsbausteinen (multi chip), oder mit allen Funktionseinheiten integriert auf einem gemeinsamen Träger (single chip).

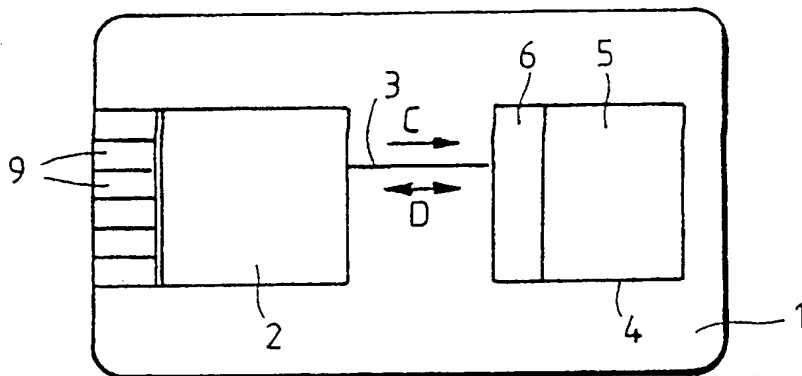


Fig. 1



Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 89 10 5509

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.5)
A	US-A-4 734 568 (WATANABE) * Spalte 8, Zeile 52 - Spalte 10, Zeile 17; Ansprüche 1, 4, 5, 8; Figuren 3-12 *	1-7	G 07 F 7 10
A	EP-A-0 152 024 (K.K. TOSHIBA) * das ganze Dokument *	1-7	
A	EP-A-0 250 309 (BULL CP8) * das ganze Dokument *	1-5	
A	FR-A-2 592 502 (LEFEVRE) * Zusammenfassung; Ansprüche 1-6; Figuren 3-9 *	1-3	
P,A	DE-A-3 736 190 (HITACHI) * das ganze Dokument *	1,3,5	
A	WO-A-8 705 420 (DATA CARD CORPORATION) * Seite 9, Zeile 1 - Seite 12, Zeile 23 *	1	
			RECHERCHIERTE SACHGEBIETE (Int. Cl.5)
			G 07 F G 06 K
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort		Abschlußdatum der Recherche	
Den Haag		21 Januar 91	
		Prüfer	
		GIVOL,O.	
KATEGORIE DER GENANNTEN DOKUMENTE			
X : von besonderer Bedeutung allein betrachtet		E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist	
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie		D : in der Anmeldung angeführtes Dokument	
A : technologischer Hintergrund		L : aus anderen Gründen angeführtes Dokument	
O : mündliche Offenbarung		& : Mitglied der gleichen Patentfamilie.	
P : Zwischenliteratur		Übereinstimmendes Dokument	
T : der Erfindung zugrunde liegende Theorien oder Grundsätze			